Table 4: The impact of Different methodology on de-obfuscation time (in seconds) along with power and area overhead for different benchmarks

Benchmarks	De-Obfuscation time using SAT-attack				Impact on Area Overhead*			Impact on Power Overhead*		
	GSHE Obf. Coverage = 10%	LUT Obf.	Proposed Obf		LUT Obf.	Proposed Obf		LUT Obf.	Proposed Obf	
			LUT + MUX	LUT + LUT		LUT + MUX	LUT + LUT		LUT + MUX	LUT + LUT
C2670	19.8	79.8	∞	∞	95.06x	7.51x	6.80x	15.14x	2.28x	1.96x
C7552	29.6	121.7	∞	∞	38.63x	3.65x	3.21x	6.39x	1.48x	1.14x
B12	31.8	150.7	∞	∞	27.56x	2.81x	2.04x	4.48x	1.41x	1.09x
FIR	745.5	28342.6	∞	∞	9.42x	1.63x	2.06x	2.62x	1.31x	1.19x
IIR	654.6	95838.4	∞	∞	8.21x	1.57x	1.36x	2.32x	1.22x	1.18x
AES	950.6	98637.5	∞	∞	11.63x	1.89x	1.59x	3.45x	1.76x	1.65x
DES	1438.7	154429	∞	∞	7.50x	1.51x	1.29x	1.90x	1.10x	1.05x

For LUT obfuscation, the size of the LUT used is 8, while proposed method (1) LUT + MUX use LUT Size 4 along with 4-MUX and (2) LUT + LUT uses LUT Size 3 with 5-LUT of Size 2 for replacing LUT Size 8. The number of gates obfuscated is reported in Table 1. However, for GSHE obfuscation 10% of gates are encrypted in random fashion. The SAT-deobfuscation time is given in seconds. * Figures represent the area and power overheads in comparison to the implementation of the circuit/design with no obfuscation.

correct configuration already programmed in. The proposed customized LUT-based solution increases the number of permutations to 2^{2^n}, where n is the size of LUT. As the side-channel attacks are compute-intensive and require precise measurements, one can argue that by achieving SAT-attack resilience, sufficient side-channel attack resilience can also be achieved. Nonetheless, there are solutions possible for integrating additional security mechanisms in place to make the aforementioned side-channel attack more difficult. The simplest option is to apply encryption to the configuration bits so that the bits given to the on-chip programmer get decrypted before being written into the LUTs. The encryption/decryption key will be generated by an on-chip PUF and is unique to each chip so it cannot be guessed or attacked. Such solutions will be integrated with the proposed customized-LUT as a part of future research.

4.4 Resiliency to Other Attacks

The proposed customized LUT-based obfuscation is also resilient to the removal attacks. One cannot remove the LUT or MUX as removing them can strip the functionality of the circuit. The layout of the LUT is visually similar and nothing can be inferred by visual inspection. Though the Electron Microscopy (EM) can be applied for read-out data during run-time, the technology is currently not mature enough to reverse engineer switching elements [11].

5 CONCLUSIONS

In this work, we have introduced obfuscation using Customized LUT to mitigate the design overhead while not compromising the security. Further, to enhance the resilience against SAT-attack and make it a practical solution, we propose to employ LUTs in conjunction with MUX that facilitates routing based obfuscation or using an extra layer of LUT for increased depth of MUX for SAT-attack, therefore, making it resilient to power analysis-based side-channel attacks and EM-based reverse engineering attacks. Our experimental results show that with the proposed customized LUT-based obfuscation, higher robustness can be achieved against SAT-attack. Furthermore, nearly 3× power and 8× area overheads can be reduced on an average, compared to the state-of-the-art defenses. LUT+MUX offer competitive resiliency compared to LUT+LUT based obfuscation while using fewer NV-elements, while LUT+LUT technique benefits the IP holder from lower design overhead perspective.

REFERENCES

[1] A. Attaran, Tyler D. Sheaves, and P. Kumar et.al. Mugula. 2018. Static Design of Spin Transfer Torques Magnetic Look Up Tables for ASIC Designs. In *GLSVLSI*.

[2] Kimia Azar, Hadi Kamali, Houman Homayoun, and Avesta Sasan. 2019. SMT Attack: Next Generation Attack on Obfuscated Circuits with Capabilities and Performance Beyond the SAT Attacks. In *Conf. on CHES*.

[3] Alex Baumgarten, Akhilesh Tyagi, and J Zambreno. 2010. Preventing IC piracy using reconfigurable logic barriers. *IEEE Design & Test of Computers* (2010).

[4] Ferdinand Brasser and et. al. 2018. Hardware-Assisted Security: Understanding Security Vulnerabilities and Emerging Attacks for Better Defenses. In *International Conference on Compilers, Architecture, and Synthesis for Embedded Systems*.

[5] R. P. Cocchi, J. P. Baukus, L. W. Chow, and B. J. Wang. 2014. Circuit camouflage integration for hardware IP protection. In *ACM/IEEE Design Automation Conf.*

[6] J. Crawford, M. Ginsberg, and et.al. Luks. 1996. Symmetry-breaking Predicates for Search Problems. In *Proceedings of the International Conference on Principles of Knowledge Representation and Reasoning*.

[7] Ramesh Karri, Jeyavijayan Rajendran, Kurt Rosenfeld, and Mohammad Tehranipoor. 2010. Trustworthy hardware: Identifying and classifying hardware trojans. *Trans. Computer* (2010).

[8] H. Mardani, K. Zamiri, and et.al. Gaj, K. 2018. LUT-Lock: A Novel LUT-Based Logic Obfuscation for FPGA-Bitstream and ASIC-Hardware Protection. In *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*.

[9] Eugene N., Alex D., and Yoav S. et.al. [n. d.]. Understanding Random SAT: Beyond the Clauses-to-Variables Ratio. In *In Proc. of CP-04*.

[10] Department of Defense. 2005. Defense science board task force on high performance microchip supply. (2005). https://www.acq.osd.mil/dsb/reports/2000s/ADA435563.pdf

[11] S. Patnaik, N. Rangarajan, and J. Knechtel et.al. 2018. Advancing hardware security using polymorphic and stochastic spin-hall effect devices. In *Design, Automation Test in Europe Conference Exhibition (DATE)*.

[12] J. Rajendran, O. Sinanoglu, and R. Karri. 2013. Is split manufacturing secure?. In *Design, Automation Test in Europe Conference Exhibition (DATE)*.

[13] A. Rezaei, Y. Shen, S. Kong, and J. Gu et.al. 2018. Cyclic locking and memristor-based obfuscation against CycSAT and inside foundry attacks. In *Design, Automation Test in Europe Conference Exhibition (DATE)*.

[14] S. Roshanisefat, H. Mardani, and A. Sasan. 2018. SRCLock: SAT-Resistant Cyclic Logic Locking for Protecting the Hardware. In *Proceedings of the 2018 on Great Lakes Symposium on VLSI*.

[15] Masoud Rostami, Farinaz Koushanfar, and Ramesh Karri. 2014. A primer on hardware security: Models, methods, and metrics. *Proc. IEEE* (2014).

[16] Hossein Sayadi, Nisarg Patel, and Sai Manoj et.al. 2018. Ensemble Learning for Effective Run-time Hardware-based Malware Detection: A Comprehensive Analysis and Classification. In *Design Automation Conference*.

[17] K. Shamsi, M. Li, and T. Meade et.al. 2017. AppSAT: Approximately deobfuscating integrated circuits. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*.

[18] Y. Shen and H. Zhou. 2017. Double DIP: Re-Evaluating Security of Logic Encryption Algorithms. In *Proceedings of the on Great Lakes Symposium on VLSI*.

[19] P. Subramanyan, S. Ray, and S. Malik. 2015. Evaluating the security of logic encryption algorithms. In *Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on*.

[20] T. Winograd, H. Salmani, and H. et.al. Mahmoodi. 2016. Hybrid STT-CMOS designs for reverse-engineering prevention. In *Proceedings of the 53rd Annual Design Automation Conference*.

[21] Y. Xie and A. Srivastava. 2017. Delay locking: Security enhancement of logic locking against IC counterfeiting and overproduction. In *ACM/EDAC/IEEE Design Automation Conference (DAC)*.

[22] Y. Xie and A. Srivastava. 2018. Anti-SAT: Mitigating SAT Attack on Logic Locking. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems* (2018).

[23] M. Yasin, B. Mazumdar, and J. J. V. Rajendran et.al. 2016. SARLock: SAT attack resistant logic locking. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*.

[24] M. Yasin, B. Mazumdar, and O. Sinanoglu et.al. 2017. Security analysis of Anti-SAT. In *Asia and South Pacific Design Automation Conference (ASP-DAC)*.

[25] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran. 2018. Removal Attacks on Logic Locking and Camouflaging Techniques. *IEEE Transactions on Emerging Topics in Computing* (2018).

[26] M. Yasin, J. J. Rajendran, and et.al. O. Sinanoglu. 2016. On Improving the Security of Logic Locking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2016).

[27] H. Zhou, R. Jiang, and S. Kong. 2017. CycSAT: SAT-based attack on cyclic logic encryptions. In *IEEE/ACM International Conference on Computer-Aided Design*.